

REMARKS

Claims 1-24 are pending in the present application. Reconsideration of the claims is respectfully requested.

I. Objection to the Drawings

The Office Action objects to the drawings under 37 CFR 1.83(a) because they allegedly do not show the feature of the selecting means and the step for selecting a list of users as recited in claims 22-24. Applicant disagrees and directs the Examiner's attention to Figure 1 of the present invention. Specifically, Figure 1 contains an Administrator Interface 22, a Profile Table 24 and a Processing Unit 20, all of which contributes to a means and step for selecting a list of users based on profile information in the profile table.

Page 4, lines 7-14 of the present specification discloses the relationship between the Administrator Interface 22 and the Profile Table 24 in selecting a list of users based on profile information in the profile table:

A message or an alarm can be manually sent when the server administrator writes the message (or alarm) on Administrator Interface 22 and initiates the transmission thereof to a list of users whose profile has been selected in Profile Table 24. Then, the message is sent by Message Sender 28 over the network to all running workstations corresponding to the selected profile. On the user workstation, the Java alarm program receives the message (or alarm) and displays it on the foreground of the user screen, and an alarm tune is also played. Once the message is read, the user presses the OK key and the program switches in the background. Then, the Java alarm program sends back to server 16 an acknowledgement which can be used for statistic purposes on the server.

In addition, page 3, lines 16-21 describe the administrator interaction with Processing Unit 20 in selecting a list of users based on profile information in the profile table:

Server 16 includes a Processing Unit 20 which handles the server and is also used to process all the operations controlled by an administrator entering the server via an administrator interface 22. Server 16 also comprises a System Network Messaging Protocol (SNMP) Interface 23 to monitor defined machines, a Profile Table 24 for the

registration of user profiles, an Alarm Scheduler 26 and a Message Sender 28 connected to node 18.

Thus, the present specification clearly states that the administrator interacts with server 16 using Administrator Interface 22. The Administrator selects users through Administrator Interface 22 from Profile Table 24. In addition, it is clear from Figure 1 and the sections reproduced above that the Processing Unit 20 allows an interaction between the Administrator Interface 22 and the Profile Table 24. Thus, the means for selecting a user resides in the Administrator Interface 22, the Processing Unit 20, or a combination of the Administrator Interface 22 and the Processing Unit 20.

Thus, despite allegations made in the Office Action, Figure 1 does, in fact, depict the feature of the selecting means and the step for selecting a list of users as recited in claims 22-24. Therefore, the objection to the drawings under 37 CFR 1.83(a) is overcome.

II. 35 U.S.C. § 112, First Paragraph

The Office Action objects to the specification under 35 U.S.C. § 112, first paragraph, as failing to adequately teach how to make and/or use the invention in claims 22-24. Additionally, the Office Action rejects the claims under the same reasons. This rejection is respectfully traversed.

In rejecting claims 22-24 under 35 U.S.C. § 112, first paragraph, the Office Action states:

The specification is objected to under 35 U.S.C. § 112, first paragraph, as failing to adequately teach how to make/or use the invention, i.e., failing to disclose list of user is a subset of the plurality of users. Applicant's disclosure is insufficient to allow one of ordinary skill in the art to make or use the invention without undue experimentation because applicant did not adequately disclose the necessary apparatus to perform the claimed method. See *In re Gunn*, 190 USPQ 402, 406 (CCPA 1976). In fact applicant's disclosure did not even sufficiently include selecting means and method step of selecting a list of users, which is a subset of the plurality of user, based on profile information in the profile table on which the claimed method and system could be implemented. Office Action dated January 29, 2004, page 2.

Applicant respectfully disagrees and directs the Examiner's attention to page 3, lines 1-8 of the present specification, which reads as follows:

Therefore, the invention relates to a system for broadcasting alarm messages from a server to a list of users among a plurality of multi-platform users sharing the server in a data transmission network operating under Internet Protocol (IP) and using the Java language. This system comprises a profile table which contains the profiles of each user, and processing and transmitting means which enable an administrator associated with the server to transmit alarm messages to the users of the list wherein the users have been selected by selecting profiles in the profile table, the alarm messages being displayed on the screen of the workstation associated with each selected user if the workstation is running.

Thus, the present specification states that the alarm message is sent to a list of users among a plurality of multi-platform users. In other words, the plurality of multi-platform users is a set of users which contains a list of users as a subset of the plurality of multi-platform users. The list of users selected from the profile table is among the plurality of multi-platform users. Thus, the present specification discloses that the list of users is a subset of the plurality of users.

In addition, as set forth above, Figure 1 of the present invention discloses the selecting means and method for selecting a list of users. Thus, the present specification does, in fact, disclose that the list of users is a subset of the plurality of users. Similarly, the present specification also discloses a selecting means and method of selecting a list of users, which is a subset of the plurality of users, based on profile information in the profile table. Therefore, the objection of the specification under 35 U.S.C. § 112, first paragraph has been overcome.

III. 35 U.S.C. § 102, Alleged Anticipation of Claims 22-24

The Office Action rejects claims 22-24 under 35 U.S.C. § 102(e) as being allegedly anticipated by Raffel et al. (U.S. Publication No. 20020082892). This rejection is respectfully traversed for at least the same reasons as noted in the Response to Office Action filed on December 17, 2003, the remarks of which are hereby incorporated by reference, with regard to claims 1, 8 and 15 from which claims 22-24 depend.

Specifically, neither Stupek nor Drala (which are the basis for the rejection of claims 1-21, from which claims 22-24 depend), either alone or in combination, teach or suggest an administrator associated with a server sending alarm messages to a list of users, selected from a plurality of users within a profile table. In addition, Raffel does not provide for the deficiencies of the proposed Stupek-Drala combination. Raffel is directed to a system for providing transactional information of deals, contracts, accounts and leads over the internet. The transactional information is accessed and shared among members of the host organization. The transactional information can be imported into other applications such as, for example, a spreadsheet. An administrator is responsible for providing each authorized user with materials necessary to use the system such as software and access information. In addition, the administrator can configure the system to notify users every time there is new or changed information for accounts or deals to which a user has access.

Thus, Raffel is concerned, in part, with notifying users when information in the system corresponding to accounts or deals is updated. While Raffel may teach sending a notification to a user, there is nothing in Raffel that teaches that an administrator associated with a server sends an alarm message to a list of users, selected from a plurality of users, within a profile table. To the contrary, the administrator in Raffel configures the system to automatically send out notifications as stated in paragraph 0082 of Raffel, which reads as follows:

The territorial configuration of the CIMS system provides a way to create groups of related accounts, contacts, and deals and to designate groups of users who have a responsibility to manage and track business taking place within each territory. In one embodiment, system administrators have the ability to establish and maintain territory definitions and to determine access rights of users to the territories, but the embodiment is not so limited. Territories are important in that they limit access to potentially sensitive deal information. By setting up territories so that they reflect the way an organization does business and by assigning appropriate staff members to each territory, only those users who are authorized to do so will be able to view or change confidential information relating to a territory. Furthermore, territories can be used to aggregate accounts and deals for reporting, filtering, and notification. For example, users may create profiles that show accounts, contacts, or deals in specific territories. Moreover, a system administrator may configure the CIMS to notify users every time there is new or changed information for accounts

or deals that are located only in their territories. This enables the member of a particular sales team to focus on the information that is most critical to them.

Thus, once the administrator selects which events will trigger a notification, the system automatically sends the notifications to the users. Claims 1, 8 and 15 of the present invention recite that the administrator sends the alarm to a list of users, selected from the plurality of users within the profile table. This is a manual process performed by an administrator and not an automatic process such as that taught in Raffel. Therefore, the rejection of claims 22-24 under 35 U.S.C. § 102(e) is overcome.

IV. 35 U.S.C. § 102, Alleged Anticipation of Claims 22-24

The Office Action rejects claims 22-24 under 35 U.S.C. § 102(e) as being allegedly anticipated by Ruckdashel et al. (U.S. Patent Mo. 6,038,542). This rejection is respectfully traversed for at least the same reasons as noted in the Response to Office Action filed on December 17, 2003 with regard to claims 1, 8 and 15 from which claims 22-24 depend.

As set forth above, neither Stupek nor Dralt (as applied to claims 1, 8 & 15), either alone or in combination, teach or suggest an administrator associated with a server sending alarm messages to a list of users, selected from a plurality of users within a profile table. In addition, Ruckdashel does not provide for the deficiencies of the proposed Stupek-Dralt combination. Ruckdashel is directed to a system for notifying an individual of a scheduled event. A server retrieves a user's schedule information and analyzes the information. Events within a specified time frame are queued and a notification server is activated at the time that the queued event is to occur. The user is then notified of the event.

As in Raffel, the process of notifying the user is automated. The administrator's main task in Ruckdashel is to maintain the database of users by adding and deleting users. The actual notification is performed by notification software. Thus, Ruckdashel does not teach an administrator associated with a server sending alarm messages to a list of users.

selected from a plurality of users, within a profile table. Therefore, the rejection of claims 22-24 under 35 U.S.C. § 102(e) is overcome.

V. Response to Examiner's Rebuttal of Applicant's Arguments With Respect to Claims 1-21

The Examiner maintains his position as set forth in the Office Action dated September 17, 2003 with regard to the rejection of claims 1-21. Specifically, the Examiner maintains the rejection of claims 1, 8 and 15 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Stupek, Jr. et al. (U.S. Patent No. 6,131,118). Additionally, the Examiner maintains the rejection of claims 2-5, 7, 9-12, 14, 16-19 and 21 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Stupek, Jr. et al. (U.S. Patent No. 6,131,118) in view of Event Notifier, a Pattern for Event Notification by Drala software published in Java Report, July 1998, Volume 3, Number 7. Further, the Examiner maintains the rejection of claims 6, 13 and 20 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Stupek, Jr. et al. (U.S. Patent No. 6,131,118) in view of Event Notifier, a Pattern for Event Notification by Drala software published in Java Report, July 1998, Volume 3, Number 7 and in further view of Cote et al. (U.S. Patent No. 6,021,262). These rejections have been addressed in the Response to Office Action filed on December 17, 2003. Thus, in the following remarks, Applicant will appropriately address only the Examiner's rebuttal of Applicant's arguments set forth in the Final Response to Office Action dated January 29, 2004.

With regard to Applicant's arguments filed on December 17, 2003, the Office Action states:

Applicant's arguments filed on 12/17/2003 have been fully considered but they are not persuasive. In the remarks, applicant argued in substance that:

(a) Prior art failed to teach administrator associated with a server sending alarm to a list of user, selected from a plurality of users within a profile table, as recited in claims 1, 8 and 15.

As to point (a), Examiner disagreed, there is no support in neither specification nor claims that suggested a list of user is or must be selected from users within a profile table. Without specific support, the examiner can interpret the claims' language as, selecting user(s) based on his or her

profiles and sending a notification to the user(s) whose profile meet a criterion. Further, the examiner noted that the claims language read on many event notification systems, e.g., contact list notification, news or services subscribing, which sent the notification on users registration, subscriptions or users profiles basis. Since, there is no specific profile structure was taught in the disclosure. The examiner, therefore, allowed to give the broadest reasonable interpretation to such claims' limitation. Furthermore, nowhere in the disclosure that suggested a list of users, i.e., user names, must be within the profile table, thus, a database contains objects' profile could be construed as a profile table. It is not necessarily that the profile table must contain list of users' name, it could be a plurality of object's profiles, which are associated with a plurality of users. Selectively, bases on a criterion, the system could form a list of users from the profiles that met the criterion, for receiving the notification(s). And, that was taught in Stupek, the interconnection engine relays a particular event based on registration information, (Col. 9, lines 1-46); in one embodiment it includes action category that includes threshold tools allow the user to be notified whenever the certain condition arise, (Col. 7, lines 10-64).

(b) The examiner hindsight.

As to point b., in response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper.

Final Office Action dated January 29, 2004, pages 5-6.

Claim 1, which is representative of claims 8 and 15 with regard to similarly recited subject matter, reads as follows:

1. System for broadcasting alarm messages from a server to a list of users among a plurality of multi-platform users sharing the server in a data transmission network operating under Internet Protocol (IP) and using Java language, said system being characterized in that it comprises:
 - a profile table containing profiles of each one of said plurality of users; and
 - processing and transmitting means enabling an administrator associated with said server to transmit alarm messages to the list of users wherein said users have been selected from said profile table, said alarm messages being displayed on a screen of a workstation associated with each selected user if said workstation is running. (emphasis added)

Stupek does not teach or suggest an administrator associated with a server sending alarm messages to a list of users, selected from a plurality of users within a profile table as recited in claims 1, 8 and 15 of the present invention. The Office Action states that there is no support in either the specification or the claims that suggests that a list of users is, or must be, selected from users within a profile table. Applicant respectfully disagrees and directs the Examiner's attention to the language of claim 1. Specifically, claim 1 recites a profile table containing profiles of each one of a plurality of users and processing and transmitting means enabling an administrator associated with said server to transmit alarm messages to the list of users wherein said users have been selected from said profile table. Thus, the profile table contains profiles for a plurality of users and alarm messages are sent to users selected from the plurality of users within the profile table.

Additionally, the present specification also provides support that the list of users is selected from users in a profile table, for example, at page 2, line 17 -- page 3, line 8, which reads as follows:

Another object of the invention is to provide a heterogeneous data transmission network such as an IP network wherein at least a server can broadcast information and alarm messages to a list of users defined by their profiles previously stored in a profile table

Therefore, the invention relates to a system for broadcasting alarm messages from a server to a list of users among a plurality of multi-platform users sharing the server in a data transmission network operating under Internet Protocol (IP) and using the Java language. This system comprises a profile table which contains the profiles of each user, and processing and transmitting means which enable an administrator associated with the server to transmit alarm messages to the users of the list wherein the users have been selected by selecting profiles in the profile table, the alarm messages being displayed on the screen of the workstation associated with each selected user if the workstation is running.

Further support for this feature is also provided at page 3, lines 1-8, which is reproduced above. This section clearly recites the feature of enabling an administrator associated with a server to transmit alarm messages to the users of the list wherein the users have been selected by selecting profiles in the profile table. Additional support can also be found at page 4, lines 7-9, which is also reproduced above. This section states that "a message or an alarm can be manually sent when the server administrator writes

the message (or alarm) on Administrator Interface 22 and initiates the transmission thereof to a list of users whose profile has been selected in Profile Table 24."

Thus, the present specification specifically recites the feature of a profile table containing profiles of a plurality of users. Additionally, the present specification also recites the feature of selecting a list of users by selecting profiles in the profile table. Thus despite allegations made in the Office Action, both the claim language and the present specification provide support for a list users being selected from users within a profile table. Therefore, the Examiner cannot simply disregard what is actually recited in the claims and come up with his own unsupported interpretation of the claim language just so it appears as though the claims read on the cited art.

In addition, the Office Action states that the present specification does not specifically recite that the profile table must contain a list of users' names. Therefore the Examiner interprets the profile table as containing a plurality of object profiles, which are associated with each of a plurality of users, wherein the system could form a list of users from profiles that meet certain criterion for receiving notifications. First, this argument is extraneous to the actual claim language. Nowhere in the claims is there any recitation of "users' names" and thus, the Examiner's arguments with regard to this topic are irrelevant. Second, even if the Examiner chooses to interpret the profile table in such a manner, Stupek still does not teach that a profile table contains a plurality of object profiles, which are associated with each of a plurality of users, wherein the system could form a list of users from profiles that meet certain criterion for receiving notifications, despite allegations made in the Final Office Action.

In Stupek, the event must meet certain criteria in order for a notification to be sent to the administrator. In the claimed invention, the users, or user profiles, must meet certain criteria in order to receive a notification. There is simply nothing in Stupek that teaches a list of users is selected based on a profile to receive an alarm message, let alone an administrator associated with a server sending alarm messages to a list of users, selected from a plurality of users within a profile table as recited in independent claims 1, 8 and 15. The Office Action, however, alleges that this feature is taught by Stupek at column 9, lines 1-46, which reads as follows:

FIG. 3 is a block diagram of the AE 210 including the interconnect engine 212 that is responsible for connecting together events with constructions or "listeners" 302 of the events. In the embodiment of FIG. 3, the interconnect engine 212 receives an event signal or notification, either externally or from a construction 302, and relays the event to the appropriate one of the constructions 302. The interconnect engine 212 determines which construction 302 to relay the particular event to based on registration information that has been recorded in the interconnect engine 212. The interconnect engine 212 includes event detection logic for registering to receive events using interconnection logic and also passes those events to the proper constructions based on the registration information. Further, the event detection logic includes a server interface for interfacing with the network and a server event handler, coupled to the server interface and the interconnection logic, that routes event notifications received by the server interface to the interconnection logic. Thus, an event cycle is supported in which the interconnect engine 212 receives an event (either externally or internally) and then determines which destination construction(s) to send the event. Next, the construction(s) may generate an internal event and the internal event is passed back to the interconnect engine 212 to begin a new cycle. This cycle is repeated as necessary for the particular management operations of the system. The SNEH 226 registers as an event forwarder and receives events for which no listener has registered.

Such unregistered events include net events received and transmitted via the HTTP server 224.

FIG. 4 is a simplified block diagram of an exemplary construction 400 according to the present invention. The construction 400 of FIG. 4 includes, but is not limited to, one or more executable components 401, interconnection data structures 402, an executable component dispatcher 403, an event receiver (or event listener proxy) 404, and executable component statistics 405. The executable components 401 enable the construction 400 to be activated by notifying the event receiver 404 of the event parameters to monitor. One or more of the executable components 401 includes an event listener component to register with the event receiver 404 and becomes a listener for one or more specific events. The event receiver 404 serves as an event proxy for the executable components 401 by registering with the interconnect engine 212 to become a listener of the one or more specific events.

This section has nothing to do with an administrator sending alarm messages to a list of users, selected from a plurality of users within a profile table. This particular section is directed to relaying events to the appropriate one of the constructions. The constructions are software components which contain one or more executable components, interconnection data structures, an executable component dispatcher, an

event receiver (or event listener proxy), and executable component statistics. The executable components within the construction contain event "listeners". The term "listener" as used in Stupek refers to a mechanism for event detection. There is nothing in this section or any other section of Stupek that teaches or suggests an administrator associated with a server sending alarm messages to a list of users, selected from a plurality of users within a profile table.

Further, the Office Action states that Stupek teaches threshold tools that allow a user to be notified whenever certain conditions arise at column 7, lines 10-64. This section, as well as surrounding text, reads as follows:

There are many categories of actions that the management server 102 discovers. One action category is hardware fault detection, which is a category of actions identifying problems with hardware. Examples of hardware fault detection include failures or predictive failures on hard drives, processors, and memory. Most problem resolutions in the hardware fault detection category are simply identified steps that the user must follow to correct the problem. Tools in this category allow viewing of the problem. Another action is software configuration actions, which are actions that identify potential problems with software configurations. Software configuration actions use version control functionality along with the concept of a "software set". The user establishes a set of software that should be loaded on a server, and this category of actions identifies any deviations from that set, and differences between the set and the latest software. Problem resolution for software configuration allows distribution of software updates, along with retrieval of new software. Tools in this category include software distribution, Internet download, and report generation.

Another action category is thresholds, which are actions that track situations on the network identified by combinations of data. The user has to configure the situations. The threshold tools allow the user to monitor management data and be notified whenever certain conditions arise. Another action category is action advisories, which are actions that notify the user whenever an event is needed to be performed, such as service advisories generated by the manufacturer of the management server 102. Other advisory examples include backups, disk storage cleanup, etc. Tools for this category provide the details of the action advisory and may allow corrective action. Another action category is software updates, which are actions that notify the user whenever a new software update to software on their network becomes available on a corresponding web site. Tools for this category allow the new update to be fetched from servers setup on a user's network. Another action category is traps, which are actions that occur when an SNMP trap, an HTTP event, a DMI indication, or similar type of trap or event is received. The trap is turned into an action that is

operated on just as any other action. The tools in this category allow the user to forward the trap to other management consoles, to page the user, provide correlation, etc.

In general, management is often classified by what is being managed: hardware, operating system, software, etc. The following Table 1 illustrates the layers and the management data that is typical of that layer. It is noted that Table 1 is by no means exhaustive and simply provides typical management data for the corresponding layer.

Thus, this section states that the management server handles action categories. One of the action categories is a threshold action category. The user configures situations for the management server to monitor. When certain conditions arise, the user is automatically notified by the system. Thus, an administrator is not sending a notification to the user. Rather, it is the management server that is automatically sending the notification to the user. Another action category is software updates. When a new software update is available, the management server automatically notifies the user that a new software update is available. Once again, there is no administrator involved in sending any type of notification to the user.

While this section of Stupek teaches the feature of allowing a user to monitor management data and then receive notification when certain conditions arise, there is absolutely nothing in this section or any other section of Stupek that teaches or suggests an administrator associated with a server sending alarm messages to a list of users, selected from a plurality of users within a profile table. This is because Stupek is not concerned with sending particular alarm messages to a list of users based on profile information. Stupek is concerned with accessing a network management server and managed devices remotely from a client system via an intranet or the Internet using a web browser. The user can specify certain criteria for the operation of the management server such as which events to monitor. There is nothing in Stupek that even alludes to an administrator sending alarm messages to a list of users, selected from a plurality of users within a profile table. As set forth above, all notifications to the user are sent automatically from the management server, not from an administrator. In other words, the users do not send notifications to themselves.

In addition, the Examiner alleges that proper hindsight reconstruction was used in rejecting the presently claimed invention. Applicant understands that all examination entails some measure of hindsight. However, when the rejection is based completely on hindsight, as in the present case, to the exclusion of what can be gleaned from the references, then the rejection is improper and should be withdrawn. As set forth above, Stupek is not even concerned with the same problems as the present invention. Stupek is directed to a system for managing a network, wherein the user interacts with a management server over the internet. The present invention, on the other hand, is concerned with determining a particular list of users from a plurality of users that may be affected by an event and having an administrator transmit an alarm message to that list of users. Thus, one of ordinary skill in the art would not even look to Stupek to solve the problems addressed in the presently claimed invention. Therefore, unless the Examiner can point to specific references that teach all of the features of the presently claimed invention, the Examiner has, indeed, used improper hindsight reconstruction to form the rejection of the presently claimed invention.

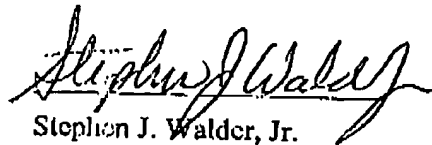
Applicant asserts that the presently claimed invention is patentable over the alleged prior art. Applicant respectfully requests withdrawal of the rejections to claims 1-24.

VI. Conclusion

It is respectfully urged that the subject application is patentable over the alleged prior art of record and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: March 29, 2004

Respectfully submitted,



Stephen J. Walder, Jr.
Reg. No. 41,534
Carstens, Yee & Cahoon, LLP
P.O. Box 802334
Dallas, TX 75380
(972) 367-2001
Attorney for Applicant

SJW/kg